

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF SOUTH DAKOTA**

---

CHRISTINE LOGAN, individually and  
on behalf of all others similarly situated;

Plaintiff,

v.

FURNITURE MART USA, INC.

Defendant.

---

4:25-cv-4018

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

**ORIGINAL COMPLAINT—CLASS ACTION**

Plaintiff Christine Logan (“Plaintiff”), individually and on behalf of all others similarly situated, sues Defendant Furniture Mart USA, Inc. (“Furniture Mart” or “Defendant”), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record.

**I. INTRODUCTION**

1. This class action arises out of the recent data security incident and data breach that was perpetrated against Defendant (the “Data Breach”), which held in its possession certain personally identifiable information (“PII” or the “Private Information”) of Plaintiff and other current and former customers of Defendant, the putative class members (“Class”). This Data Breach occurred November 3, 2024.

2. The Private Information compromised in the Data Breach included certain personal or protected information of Defendant’s customers, including Plaintiff. This Private Information

included but is not limited to “name, Social Security number, and driver’s license or state identification number.”<sup>1</sup>

3. Defendant has reported to the Maine Attorney General’s office that the Data Breach affected 9,718 individuals.<sup>2</sup>

4. The Data Breach resulted from Defendant’s failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals’ Private Information with which it was entrusted for business relationships.

5. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant’s inadequate safeguarding of Class Members’ Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information was subjected to unauthorized access by an unknown third party and precisely what type of information was accessed.

6. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant’s computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff’s and Class Members’ Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

7. Defendant, through its employees, disregarded the rights of Plaintiff and Class Members (defined below) by, among other things, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were

---

<sup>1</sup> Office of the Maine Attorney General, Data Breach Notifications, *available at* <https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/fa4db5b5-edf2-4a1c-98bb-d018ffae45.html> (*last accessed* February 3, 2025).

<sup>2</sup> *Id.*

protected against unauthorized intrusions. Defendant also failed to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff's and Class Members' Private Information and failed to take standard and reasonably available steps to prevent the Data Breach.

8. In addition, Defendant failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant's employees (presumably in the IT department) properly monitored its property, it would have discovered the intrusion sooner.

9. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

10. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes. These crimes include opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

11. Because of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and ongoing risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

12. Plaintiff and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

13. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

14. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

15. Accordingly, Plaintiff sues Defendant seeking redress for their unlawful conduct, and asserting claims for: (i) negligence, (ii) breach of implied contract, (iii) breach of fiduciary duty, and (iv) unjust enrichment.

## **II. PARTIES**

16. Plaintiff Christine Logan is and at all times mentioned herein was an individual citizen of South Dakota, residing in the city of Sioux Falls.

17. Plaintiff provided Defendant with her sensitive PII as part of buying goods from Defendant. Plaintiff received notice of the Data Breach around January 24, 2025, informing her that her sensitive information was part of Defendant's Data Breach.

18. Defendant Furniture Mart USA, Inc. is a furniture retailer with over 50 retail locations in six Midwest states. Defendant's principal place of business is 140 E. Hinks Lane, Sioux Falls, South Dakota 57104. Defendant's registered agent for service of process is William A. Hinks, 140 E. Hinks Lane, Sioux Falls, South Dakota 57104.

## **III. JURISDICTION AND VENUE**

19. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of

interest and costs. The number of class members exceeds 100, many of whom have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

20. This Court has general personal jurisdiction over Defendant because Defendant is based and operates in the District of South Dakota.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is based in this District, maintains Plaintiff's and Class Members' Private Information in this District, and has caused harm to Plaintiff and Class Members in this District.

#### **IV. FACTUAL ALLEGATIONS**

##### ***Defendant's Business***

22. Defendant Furniture Mart USA, Inc., is a South Dakota furniture retailer that sells goods to customers in South Dakota, North Dakota, Iowa, Illinois, Wisconsin and Minnesota.

23. In the ordinary course of selling goods, each customer must provide (and Plaintiff did provide) Defendant with sensitive, personal, and private information, such as his or her name, Social Security number, and driver's license or state identification number.

24. Defendant agreed to and undertook legal duties to maintain the Private Information entrusted to it by Plaintiff and Class Members safely, confidentially, and in compliance with all applicable laws.

25. The customer information held by Defendant in its computer system and network included the Private Information of Plaintiff and Class Members.

##### ***The Data Breach***

26. A Data Breach occurs when cyber criminals intend to access and steal Private Information that has not been adequately secured by a business entity like Defendant.

27. According to the Notice of Data Breach Defendant provided to the Maine Attorney General's office,

**What Happened?** On November 3, 2024, Furniture Mart became aware of suspicious activity involving our systems and promptly began an investigation. On December 2, 2024, the investigation determined that an unknown actor viewed and copied certain files from our systems on November 3, 2024. We are reviewing our records to identify individuals whose personal information was involved in this event and locate address information for those individuals. While the review is ongoing, on December 26, 2024, we identified address information for certain individuals with personal information involved in this event.

28. Defendant had obligations created by contract, industry standards, common law, and representations made to Class Members, to keep Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

29. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

30. Defendant was or should have been aware of the significant risk that cybercriminals would attempt to steal Plaintiff's and Class Members' Private Information.

31. As reported by the Identity Theft Resource Center, in 2023 a record 3,205 data breaches occurred, resulting in around 353,027,892 individuals' information being compromised, a 78% increase from 2022.<sup>3</sup> Of the 2023 recorded data breaches, 119 of them, or close to 4%, were in the retail industry.<sup>4</sup>

---

<sup>3</sup> See Identity Theft Resource Center, *2023 Data Breach Report* (January 2024), available at [https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC\\_2023-Annual-Data-Breach-Report.pdf](https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf) (last visited February 3, 2025).

<sup>4</sup> *Id.*

32. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

***Defendant Failed to Comply with FTC Guidelines***

33. The Federal Trade Commission ("FTC") has promulgated many guides for businesses which show how important it is to implement reasonable data security practices. According to the FTC, the need for data security should shape all business decision-making.

34. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.<sup>5</sup> The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor incoming traffic for activity suggesting someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.<sup>6</sup>

35. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

---

<sup>5</sup> Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (2016), available at [www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](http://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last visited February 3, 2025).

<sup>6</sup> *Id.*

36. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect client data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions also clarify the measures businesses must take to meet their data security obligations.

37. Defendant failed to properly implement basic data security practices. Defendant’s failure to employ reasonable and appropriate measures to protect against unauthorized access to customers’ PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

38. Defendant was always fully aware of its obligation to protect the PII of its customers. Defendant was also aware of the significant repercussions that would result from its failure to do so.

***Defendant Failed to Comply with Industry Standards***

39. As shown above, retailers are widely known to be particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

40. Several best practices have been identified that at a minimum should be implemented by retailers like Defendant, including, but not limited to, educating all employees; strong passwords; multi-layer security, including firewalls, antivirus, and antimalware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

41. Other best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and



routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

42. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including, without limitation, PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

43. These foregoing frameworks are existing and applicable industry standards for any business that handles and stores large volumes of sensitive information, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

## **V. DEFENDANT'S BREACH**

44. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and its data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;
- b. Failing to adequately protect customers' Private Information;
- c. Failing to properly monitor its own data security systems for existing intrusions;
- d. Failing to train employees in the proper handling of emails containing malicious software, and to and maintain adequate email security practices;
- e. Failing to put into place proper procedures, software settings, and data security software protections to adequately protect against a blunt force intrusion;
- f. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and

g. Failing to adhere to industry standards for cybersecurity.

45. As the result of computer systems needing security upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, and inadequately trained employees who opened files containing the ransomware virus, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

46. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft.

***Because of Defendant's Failure to Safeguard Private Information, Plaintiff and the Class Members Have and Will Experience Substantial Harm in the Form of Risk of Continued Identity Theft.***

47. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

48. The ramifications of Defendant's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes. According to experts, one out of four data breach notification recipients become a victim of identity fraud.

49. Because of Defendant's failures to prevent—and to timely detect—the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

- a. The loss of the opportunity to control how their PII is used;
- b. The diminution in value of their PII;
- c. The compromise and continuing publication of their PII;
- d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

- e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;
- f. Delay in receipt of tax refund monies;
- g. Unauthorized use of stolen PII; and
- h. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

50. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to \$1,000.00 depending on the type of information obtained.

51. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals often post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

52. It can take victims years to spot identity or PII theft, giving criminals plenty of time to milk that information for cash.

53. One such example of criminals using PII for profit is the development of "Fullz" packages.

54. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

55. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain

information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII is being misused, and that such misuse is traceable to the Data Breach.

56. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than \$3.5 billion in losses to individuals and business victims, and the numbers are only rising.

57. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good" Defendant did not rapidly report to Plaintiff and the Class that their PII had been stolen.

58. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

59. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

60. Further complicating the issues faced by victims of identity theft, data thieves may

wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

61. The Federal Trade Commission (“FTC”) has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that “most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency.”<sup>7</sup>

62. The FTC has also issued many guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires:

- (1) encrypting information stored on computer networks;
- (2) retaining payment card information only as long as necessary;
- (3) properly disposing of personal information that is no longer needed;
- (4) limiting administrative access to business systems;
- (5) using industry-tested and accepted methods for securing data;
- (6) monitoring activity on networks to uncover unapproved activity;
- (7) verifying that privacy and security features function properly;
- (8) testing for common vulnerabilities; and
- (9) updating and patching third-party software.

63. According to the FTC, unauthorized PII disclosures ravage consumers’ finances,

---

<sup>7</sup> Statement of FTC Commissioner Pamela Jones Harbour-Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009), <http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf> (last visited February 3, 2025).

credit history and reputation, and can take time, money and patience to resolve the fallout.<sup>8</sup> The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

64. Defendant's failure to properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff's and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

## **VI. PLAINTIFF'S EXPERIENCE**

65. Plaintiff Christine Logan is and at all times mentioned herein was an individual citizen of South Dakota, residing in the city of Sioux Falls.

66. Plaintiff was a customer of Furniture Mart, requiring her to provide her Private Information to Defendant.

67. After Plaintiff provided Private Information, Defendant suffered a Data Breach.

68. Plaintiff reasonably expected and understood that Defendant would take, at a minimum, industry standard precautions to protect, maintain, and safeguard her Private Information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to the same. Plaintiff would not have provided her Private Information to Defendant had she known that Defendant would not take reasonable steps to safeguard it.

69. Plaintiff is very careful about sharing her sensitive PII. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff also

---

<sup>8</sup> See Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), *available at* <https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen> (last visited February 3, 2025).

stores any documents containing her sensitive information in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for online accounts containing sensitive information.

70. Plaintiff received a notice from Defendant around January 24, 2025, stating that her Private Information may have been compromised in the Data Breach.

71. Because of the Data Breach and at the recommendation of Defendant and its Notice, Plaintiff made reasonable efforts to mitigate the effect of the Data Breach, including, but not limited to, researching the Data Breach and monitoring her credit and financial statements.

72. Plaintiff has spent much time responding to the dangers from the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to work and recreation.

73. Even with the best response, the harm caused to Plaintiff cannot be undone.

74. Plaintiff knows that cybercriminals often sell Private Information, and that her PII could be abused months or even years after a data breach.

75. Had Plaintiff been aware that Defendant's computer systems were not secure, she would not have entrusted Defendant with her personal data.

## **VII. PLAINTIFF'S AND CLASS MEMBERS' DAMAGES**

76. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered because of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach. Defendant has only offered 12 months of inadequate credit monitoring services, despite Plaintiff and Class Members being at risk of identity theft and fraud for the remainder of their lifetimes.

77. The credit monitoring offered to persons whose Private Information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches

and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud.

78. Defendant's credit monitoring advice to Plaintiff and Class Members places the burden on Plaintiff and Class Members, rather than on Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach.

79. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

80. Plaintiff's Private Information was compromised and exfiltrated by cybercriminals as a direct and proximate result of the Data Breach.

81. Plaintiff was damaged in that her Private Information is in the hands of cybercriminals.

82. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an actual, present, immediate, and continuing increased risk of harm from fraud and identity theft.

83. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

84. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

85. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential



fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

86. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

87. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Many courts have recognized the propriety of loss of value damages in related cases.

88. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

89. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

- a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;
- b. Purchasing credit monitoring and identity theft prevention;
- c. Placing “freezes” and “alerts” with reporting agencies;
- d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;
- e. Contacting financial institutions and closing or modifying financial accounts; and
- f. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

90. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by implementing security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information is inaccessible online and that access to such data is password protected.

91. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

### **VIII. CLASS ACTION ALLEGATIONS**

92. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure.

93. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

**All persons whose Private Information was compromised because of the November 2024 Data Breach (the "Class").**

94. Excluded from the Class are Defendant's officers and directors, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and members of their staff.

95. Plaintiff reserves the right to amend or modify the class definitions with greater specificity or division after having an opportunity to conduct discovery.

96. Numerosity. The Members of the Class are so numerous that joinder of all of them in a single proceeding is impracticable. The exact number of Class Members is unknown to

Plaintiff now, but Defendant has reported to the Maine Attorney General that 9,718 individuals were affected by the Data Breach.

97. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;
- b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- d. Whether Defendant's data security systems prior to and during the Data Breach adhered to industry standards;
- e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;
- f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;
- g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- h. Whether Plaintiff and Class Members suffered legally cognizable damages from Defendant's misconduct;
- i. Whether Defendant failed to provide notice of the Data Breach promptly; and
- j. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

98. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, among other things, all Class Members were injured through the common misconduct of Defendant.

Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members, and no defenses are unique to Plaintiff. Plaintiff's claims and those of Class Members arise from the same operative facts and are based on the same legal theories.

99. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

100. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

101. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy.

102. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

103. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

104. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

## **IX. CAUSES OF ACTION**

### **FIRST COUNT NEGLIGENCE**

#### **(On Behalf of Plaintiff and All Class Members)**

105. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

106. Defendant required Plaintiff and Class Members to submit non-public personal information to do business with Furniture Mart.

107. By collecting and storing this data in Defendant's computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period and to give prompt notice to those affected in the case of a Data Breach.

108. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

109. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, a necessary part of obtaining services from Defendant.

110. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

111. Defendant further had a duty to use reasonable care in protecting confidential data because Defendant is bound by industry standards to protect confidential Private Information.

112. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- b. Failing to adequately monitor the security of its networks and systems;
- c. Failing to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;
- d. Allowing unauthorized access to Class Members' Private Information;
- e. Failing to detect timely that Class Members' Private Information had been compromised;
- f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and
- g. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

113. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

114. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

115. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

116. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner.

117. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate credit monitoring to all Class Members.

**SECOND COUNT  
BREACH OF IMPLIED CONTRACT  
(On Behalf of Plaintiff and All Class Members)**

118. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

119. When Plaintiff and Class Members provided their Private Information to Defendant in exchange for Defendant's services, they entered implied contracts with Defendant under which Defendant agreed to reasonably protect such information.

120. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

121. In entering such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and adhered to industry standards.

122. Plaintiff and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

123. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

124. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that they adopted reasonable data security measures.

125. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

126. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

127. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged here, including the loss of the benefit of the bargain.

128. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered because of the Data Breach.

129. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit



to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

**THIRD COUNT  
BREACH OF FIDUCIARY DUTY  
(On Behalf of Plaintiff and All Class Members)**

130. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

131. Defendant became guardian of Plaintiff's and Class Members' Private Information, creating a special relationship between Defendant and Plaintiff and Class Members.

132. As such, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

133. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with its and account holders, in particular, to keep secure their Private Information.

134. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

135. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

136. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

137. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to:

- a. actual identity theft;
- b. the compromise, publication, and/or theft of their Private Information;
- c. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information;
- d. lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft;
- e. the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession;
- f. future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the rest of the lives of Plaintiff and Class Members; and
- g. the diminished value of Defendant's services they received.

138. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

**FOURTH COUNT  
UNJUST ENRICHMENT  
(On Behalf of Plaintiff and All Class Members)**

139. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

140. Plaintiff brings this claim individually and on behalf of all Class Members. This count is pled in the alternative to the breach of contract count above.

141. Upon information and belief, Defendant funds its data security measures entirely from its general revenue.

142. As such, a portion of the revenue attributable to Plaintiff's and Class Members' purchases is to be used to provide a reasonable level of data security, and the portion of those revenues that is allocated to data security is known to Defendant.

143. Plaintiff and Class Members conferred a monetary benefit on Defendant. They engaged in business with Defendant and in so doing provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have received from Defendant the services that were the subject of the transaction and appropriate protection for their Private Information.

144. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

145. Defendant enriched itself by saving the costs Defendant reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Rather than providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by using cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

146. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

147. Defendant failed to secure Plaintiff's and Class Members' Private Information and thus did not provide full compensation for the benefit Plaintiff and Class Members provided.

148. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices alleged.

149. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

150. Plaintiff and Class Members have no adequate remedy at law.

151. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to:

- a. actual identity theft;
- b. the loss of the opportunity to control how their Private Information is used;
- c. the compromise, publication, and/or theft of their Private Information;
- d. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information;
- e. lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft;
- f. the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and
- g. future costs in terms of time, effort, and money to be expended to prevent, detect, contest, and repair the effect of the Private Information compromised because of the Data Breach for the rest of the lives of Plaintiffs and Class Members.

152. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

153. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them.

## **X. PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, on behalf of herself and the Class described above seeks the following relief:

- a. For an Order certifying this action as a class action, defining the Class as requested herein, appointing Plaintiff and her counsel to represent the Class, and finding that Plaintiff is a proper representative of the Class requested herein;
- b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein relating to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;
- c. For equitable relief compelling Defendant to use appropriate methods and policies related to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;
- d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained because of Defendant's wrongful conduct;
- e. For an Order directing Defendant to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;
- f. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
- g. For an award of punitive damages, as allowable by law;
- h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- i. Pre- and post-judgment interest on any amounts awarded; and
- j. Any other relief that this court may deem just and proper.

**XI. JURY TRIAL DEMANDED**

Plaintiff demands a trial by jury on all claims so triable.

Dated: February 5, 2025

Respectfully submitted,

/s/ Brett Waltner

Brett Waltner  
Myers Billion, LLP  
230 S. Phillips Ave. Ste. 300  
Sioux Falls, SD 57104  
Tel: (605) 336-3700  
[bwaltner@myersbillion.com](mailto:bwaltner@myersbillion.com)

/s/ Leigh S. Montgomery

Leigh S. Montgomery\*

Texas Bar No. 24052214

**EKSM, LLP**

4200 Montrose Blvd., Suite 200

Houston, Texas 77006

Phone: (888) 350-3931

Fax: (888) 276-3455

[lmontgomery@eksm.com](mailto:lmontgomery@eksm.com)

**ATTORNEYS FOR PLAINTIFF**

(\* denotes *pro hac vice* forthcoming)

## CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

**I. (a) PLAINTIFFS**

(b) County of Residence of First Listed Plaintiff \_\_\_\_\_  
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

**DEFENDANTS**

County of Residence of First Listed Defendant \_\_\_\_\_  
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

**II. BASIS OF JURISDICTION** (Place an "X" in One Box Only)

- ☐ 1 U.S. Government Plaintiff ☐ 3 Federal Question (U.S. Government Not a Party)
- ☐ 2 U.S. Government Defendant ☐ 4 Diversity (Indicate Citizenship of Parties in Item III)

**III. CITIZENSHIP OF PRINCIPAL PARTIES** (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- |   | PTF                        | DEF                        |   | PTF                        | DEF                        |
|---|----------------------------|----------------------------|---|----------------------------|----------------------------|
| Citizen of This State                   | <input type="checkbox"/> 1 | <input type="checkbox"/> 1 | Incorporated or Principal Place of Business In This State     | <input type="checkbox"/> 4 | <input type="checkbox"/> 4 |
| Citizen of Another State                | <input type="checkbox"/> 2 | <input type="checkbox"/> 2 | Incorporated and Principal Place of Business In Another State | <input type="checkbox"/> 5 | <input type="checkbox"/> 5 |
| Citizen or Subject of a Foreign Country | <input type="checkbox"/> 3 | <input type="checkbox"/> 3 | Foreign Nation  | <input type="checkbox"/> 6 | <input type="checkbox"/> 6 |

**IV. NATURE OF SUIT** (Place an "X" in One Box Only)

Click here for: [Nature of Suit Code Descriptions.](#)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	<b>PERSONAL INJURY</b> <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Medical Malpractice <b>PERSONAL INJURY</b> <input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability <b>PERSONAL PROPERTY</b> <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 690 Other <b>LABOR</b> <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Management Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act <b>IMMIGRATION</b> <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 <b>INTELLECTUAL PROPERTY RIGHTS</b> <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 835 Patent - Abbreviated New Drug Application <input type="checkbox"/> 840 Trademark <input type="checkbox"/> 880 Defend Trade Secrets Act of 2016 <b>SOCIAL SECURITY</b> <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) <b>FEDERAL TAX SUITS</b> <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609	<input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 376 Qui Tam (31 USC 3729(a)) <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit (15 USC 1681 or 1692) <input type="checkbox"/> 485 Telephone Consumer Protection Act <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes
<b>REAL PROPERTY</b> <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	<b>CIVIL RIGHTS</b> <input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input type="checkbox"/> 448 Education <b>PRISONER PETITIONS</b> <b>Habeas Corpus:</b> <input type="checkbox"/> 463 Alien Detainee <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty <b>Other:</b> <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement			

**V. ORIGIN** (Place an "X" in One Box Only)

- ☐ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District (specify) ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

**VI. CAUSE OF ACTION**

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):

Brief description of cause:

**VII. REQUESTED IN COMPLAINT:**

☐ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P. **DEMAND \$**

CHECK YES only if demanded in complaint:

**JURY DEMAND:** ☐ Yes ☐ No

**VIII. RELATED CASE(S) IF ANY**

(See instructions):

JUDGE \_\_\_\_\_ DOCKET NUMBER \_\_\_\_\_

DATE

SIGNATURE OF ATTORNEY OF RECORD

**FOR OFFICE USE ONLY**

RECEIPT # \_\_\_\_\_ AMOUNT \_\_\_\_\_ APPLYING IFP \_\_\_\_\_ JUDGE \_\_\_\_\_ MAG. JUDGE \_\_\_\_\_

**INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44**

## Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I.(a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
  - (b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)
  - (c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".
- II. Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
- United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here. United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
- Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
- Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: [Nature of Suit Code Descriptions](#).
- V. Origin.** Place an "X" in one of the seven boxes.
- Original Proceedings. (1) Cases which originate in the United States district courts.
- Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
- Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
- Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
- Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
- Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
- Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
- PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7.** Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.
- VII. Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
- Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
- Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS 44 is used to reference related cases, if any. If there are related cases, insert the docket numbers and the corresponding judge names for such cases.

**Date and Attorney Signature.** Date and sign the civil cover sheet.